(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号

特開平10－21305

(43)公開日　平成10年(1998)１月23日

(51)Int.Cl.[6]	識別記号	庁内整理番号	ＦＩ		技術表示箇所
Ｇ０６Ｆ　17/60			Ｇ０６Ｆ　15/21	３３０	
Ｇ０６Ｔ　7/00			Ｈ０４Ｍ　3/42	Ｚ	
Ｈ０４Ｍ　3/42			Ｇ０６Ｆ　15/21	３４０Ｂ	
			15/62	４６５Ｕ	

審査請求　未請求　請求項の数２　ＦＤ　（全９頁）

(21)出願番号　特願平8－188055

(22)出願日　平成８年(1996)７月１日

(71)出願人　000005810
日立マクセル株式会社
大阪府茨木市丑寅１丁目１番88号

(72)発明者　中村　昂
大阪府茨木市丑寅一丁目１番88号　日立マクセル株式会社内

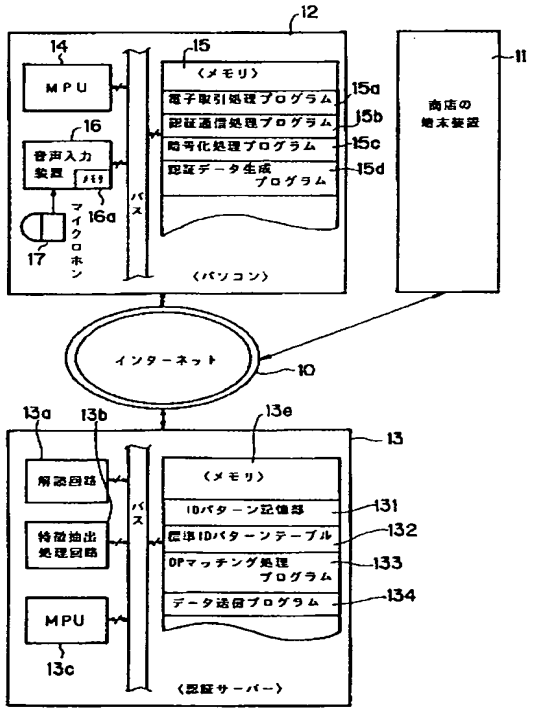
(74)代理人　弁理士　梶山　佶是　（外１名）

(54)【発明の名称】　電子商品取引システム

(57)【要約】　（修正有）

【課題】より安全性の高い本人確認ができる電子商品取引システムを提供する。

【解決手段】インターネット１０に接続され、商品購入の情報を受信する商店の端末装置１１と、商品の購入者固有の身体的特徴の情報とこれを検索するための検索コードとを商品購入の情報に付加して認証サーバ１３に送信する情報処理装置１２とからなる。認証サーバ１３は購入者固有の身体的特徴の情報を被照合情報として検索コードに対応させて記憶しているメモリ１３ｅを有し、情報処理装置１２から送出された身体的特徴と検索コードと商品購入の情報とを受けて検索コードにより検索した身体的特徴の情報との一致の有無を判定して、それらが一致しているときに、商店の端末装置１１に商品購入についての情報を送出する。



1

【特許請求の範囲】

【請求項１】ネットワークに接続された情報処理装置を利用して商品の売買を行う電子商品取引システムにおいて、

前記ネットワークに接続され、前記商品の販売情報を前記ネットワークを介して送出し、所定の商品購入についての情報を受信する第１の情報処理装置と、

前記ネットワークに接続され、前記商品の販売情報を受信して前記商品の購入の処理を行いかつ購入者固有の身体的特徴の情報とこれを検索するための検索コードとを前記商品購入についての情報に付加して特定の認証装置に送信する第２の情報処理装置と、

前記特定の認証装置として前記ネットワークに接続され、多数の購入者固有の身体的特徴の情報を被照合情報としてそれぞれに対応する検索コードにより検索できる状態で記憶している記憶媒体を有し、前記第２の情報処理装置から送出された身体的特徴の情報と前記検索コードと前記商品購入についての情報とを受けて受けた検索コードにより前記記録媒体を検索して得られる被照合情報と前記受信した身体的特徴の情報との一致の有無を判定してそれらが一致しているときに、前記第１の情報処理装置に前記商品購入についての情報を送出する第３の情報処理装置とを備える電子商品取引システム。

【請求項２】前記ネットワークはインターネットであり、前記第３の情報処理装置は、前記記憶媒体に前記商品を取り扱う商品取扱者固有の身体的特徴の情報を被照合情報としてこれの検索コードとともにさらに有していて、前記第２の情報処理装置から前記受信した身体的特徴の情報との一致の有無を判定してそれらが一致しているときに、前記第１の情報処理装置に対して前記商品取扱者の身体的特徴の情報と前記これの検索コードとの送信を要求し、前記第１の情報処理装置から送出された身体的特徴の情報と前記第１の情報処理装置から送出された前記検索コードとを受けて受けた検索コードにより前記記録媒体を検索して得られる被照合情報と前記受信した身体的特徴の情報との一致の有無を判定してそれらが一致しているときに、前記第１の情報処理装置に前記商品購入についての情報を送出し、少なくとも前記第２の情報処理装置から前記第３の情報処理装置における伝送データが暗号化されている請求項１記載の電子商品取引システム。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】この発明は、電子商品取引システムに関し、詳しくは、インターネット等の公衆回線を介してコンピュータを利用して商品の購入を行い、個人認証をして代金の決済を行う電子商品取引システムにおいて、信頼性の高い本人認証を行うことができるような電子商品取引システムに関する。

【０００２】

2

【従来の技術】電子商品取引システムの１つとして、ディスクトップ型やノート型のパーソナルコンピュータ（以下パソコン）等を使用してインターネットに接続し、インターネット経由で所定のサービス会社のホームページに接続し、ホームページのサービス項目から、例えば、レストランの予約を選択し、日時、人数、料理コースなどを入力することでレストランの予約をするシステムがある。さらに、このような予約のほかに、宿泊施設の予約、そして商品の購入も同様に特定の会社のホームページを閲覧してそのサービス項目から順次選択することで行われ、商品については、特定の商品が映像化され、画面上に表示された商品を選択し、選択した商品について商品番号、単価、数量等を入力して購入することが行われている。しかも、最近では、このような購入がパソコンを越えてＰＤＡ（携帯用情報通信端末）やこれに接続された簡易型携帯電話（ＰＨＳ）などを使用する電子取引システムも提案されている。

【０００３】このような電子商品取引システムにおいては、代金の決済に応じて、通常、クレジット会社や銀行から個人認証した個人や法人の口座から商品代金が引き落とされ、支払いが行われる。そこで、重要になるのは、購入者あるいは予約者の本人認証である。従来のこの種の認証には、ＩＣカードが用いられ、これによる個人認証が行われて決済がなされる。特に最近では、前記の商品取引に応じて即座に決済が行われるオンライン決済も提案されている。インターネットを利用してのオンライン決済の１つとして、例えば、ＩＣカード等を利用してインターネット上の接続会員のデータ管理を行うプロバイダの認証サーバーに送って、これにより個人認証をし、さらに前記のＩＣカードにより認証サーバーとＩＣカードとの確認情報をクレジット会社あるいは販売管理会社に設けられたサーバーに送って、これによりさらに認証確認をするという二重の確認処理により安全性の高い認証を行うシステムが提案されている。

【０００４】図６は、予約販売会社とプロバイダーとの二重確認についての説明図である。まず、インターネット１０上で接続された予約販売会社のサーバー１とパソコン２とが接続されて予約商品の選択が終了すると、パソコン２にＩＣカード３を装着して暗唱コードを入力する。ＩＣカード３の情報と暗唱コードとが照合されるとともに、インターネット１０を介してプロバイダの認証サーバー４に送出されてここでも個人認証が行われ、ＩＣカード３に返される。このとき、認証サーバー４からパソコン２に本人であることとブラックリストとの照合結果などの所定の確認データが送出され、パソコン２に転送される。次に、パソコン２上の所定のキーを入力すると、インターネット１０上を介してパソコン２が予約サーバー１に対して認証サーバー４とＩＣカード３とによる交信結果データと予約情報と暗唱コード等が送出される。予約サーバー１に送信されたそれぞれの情報につ

いてさらにＩＣカード３との間で確認処理がなされた上で、予約処理が実行される。その結果、双方のサーバーで確認が採れたときに、クレジット会社５に金額決済のデータを送出し、会員の口座から代金が引き落とされる。もちろん、このとき、ＩＣカード３の情報、暗唱コード、個人確認結果のデータ等は所定のスクランブル処理（あるいは暗号化処理）がなされ、これらのデータを受信した側はスクランブルの解除（あるいは解読処理）をすることになる。

【０００５】

【発明が解決しようとする課題】電子商品取引システムは、このような特定のサービス会社を通す予約の場合ばかりでなく、個人商店や大小各種の会社がインターネット上でホームページを設けて、仮想商店により、商品の販売を行い、自由に販売商品の選択ができるようになっている。このような商店に対してそれぞれ予約サーバーに対応するような大きなシステムを設けることはできない。だからと言って、プロバイダによる認証だけでは安全性が低い。また、前記の個人認証は、ＩＣカードによるものであり、単に個別の認証処理を認証サーバー２つにより重ねているものであって、二重の認証といっても、それぞれのサーバーが個別に入力された暗唱コードとＩＣカードからのデータに基づいて個人認証を行うシステムであることには変わりがない。しかも、暗唱コードは、操作中に盗み見られたり、生年月日などから容易に推定されて危険性が高く、ＩＣカートの特定のコードは、データ量が少ないので、インターネット上を流れるときにハッカにより解読されてしまう危険性が高い。ＩＣカードのシステムが解読されてしまえば、二重化した意味もなくなる。したがって、インターネット等の公衆に解放されたネットワークにおいて金額決済を含む電子商品取引システムでは、より安全性の高い本人確認が必要である。この発明は、このような従来技術の問題点に鑑みなされたものであり、より安全性の高い本人確認ができる電子商品取引システムを提供することを目的とする。

【０００６】

【課題を解決するための手段】このような目的を達成するためのこの発明の電子商品取引システムの特徴は、ネットワークに接続された情報処理装置を利用して商品の売買を行う電子商品取引システムにおいて、ネットワークに接続され、商品の販売情報をネットワークを介して送出し、所定の商品購入についての情報を受信する第１の情報処理装置と、ネットワークに接続され、商品の販売情報を受信して商品の購入の処理を行いかつ購入者固有の身体的特徴の情報とこれを検索するための検索コードとを商品購入についての情報に付加して特定の認証装置に送信する第２の情報処理装置と、特定の認証装置として前記ネットワークに接続され、多数の購入者固有の身体的特徴の情報を被照合情報としてそれぞれに対応する検索コードにより検索できる状態で記憶している記憶媒体を有し、第２の情報処理装置から送出された身体的特徴の情報と検索コードと商品購入についての情報とを受けて受けた検索コードにより記録媒体を検索して得られる被照合情報と受信した身体的特徴の情報との一致の有無を判定してそれらが一致しているときに、第１の情報処理装置に商品購入についての情報を送出する第３の情報処理装置とを備えるものである。

【０００７】

【発明の実施の形態】前記のように、この発明にあっては、本人確認のために、暗唱コードなどのパスワードを用いずに身体的特徴を用いることで、認証のためのデータ量が多くなる。それだけ認証データの解読がし難くなる。また、身体的特徴である関係からその人特有の情報になる。さらに、認証サーバー等の第３の情報処理装置に第三者機関として配置し、身体的特徴の情報を認証情報として商品購入情報と合わせて伝送するようにしている。このようにすることで、商品取引と本人確認とが第三者機関を介在して行われることになるので信頼性が増加する。特に、身体的特徴の情報と検索コードの伝送情報は、第２の情報処理装置（商品購入者）から第３の情報処理装置（認証サーバー）と一方的に流れる伝送になっていて、さらに、購入情報も第３の情報処理装置（認証サーバー）から第１の情報処理装置と一方的に流れる伝送である。したがって、商品購入者と認証サーバーとの間だけで特殊な暗号化によりデータ送信ができる。また、商品の販売者（商品取扱者）と認証サーバーとの間でも必要な場合には別な暗号化も可能であり、ここでは購入者の身体的特徴の情報や検索コードの情報伝送は不要になる。その結果、ＩＣカードのように、第１の情報処理装置と第２の情報処理装置あるいは第３の情報処理装置と第２の情報処理装置との間で個人確認されたことについてのデータの授受をしなくても済むので、信頼性が向上する。さらに、前記の一方向の伝送により購入者と商店との直接的な接続が関係が切り離されるので、誰がどの商品をどの商店から購入するのか、その関係が分かり難くなる。それだけ情報の解読がし難くなるので、商品取引に対する信頼性が向上する。また、専用に第３の情報処理装置を認証のために設けているので、ＩＣカードに比べて確認データを大きな情報量で扱うことができ、例えば、声紋や、角膜紋、指紋、指の骨形状、顔面パターンなどをより解読が難しい確認データを利用することもできる。特に、第３の情報処理装置（認証サーバー）から第１の情報処理装置（商店側）に対しても同じように身体的特徴の情報と検索コードの伝送を要求して第３の情報処理装置で確認してから購入情報を第１の情報処理装置に送出するようにすれば、購入者側の安全性も保証される。

【０００８】

【実施例１】図１は、この発明の電子商品取引システム

のインターネットを利用した一実施例のブロック図であり、図２は、電子取引処理の購入者側装置の処理のフローチャート、図３は、電子取引における商品購入フォーマットの一例の説明図、図４は、電子取引処理における認証サーバーの処理のフローチャート、そして、図５は、インターネットを利用した電子商品取引システムの全体的な構成図である。なお、図６に示すものと同一の構成要素は同一の符号で示す。図５において、１１は、インターネット１０に接続されたインターネットに接続されるホームページを有するある商品を販売するある商店の端末装置（仮想商店）であり、１２は、商店の端末装置１１からある商品を購入するインターネット１０に接続された個人のパソコンである。１３は、インターネット１０に接続された認証サービス会社の認証サーバーである。なお、６は、インターネットとの接続を管理しているプロバイダである。認証サーバー１３は、特定のプロバイダ６とは関係なしに、商店の端末装置１１や個人のパソコン１２と同様に第三者として単にインターネット１０に接続されているものである。

【０００９】ここで、パソコン１２には、図１に示されるように、ＭＰＵ１４とメモリ１５、そして、音声入力装置１６、マイクロホン１７等を有していてる。音声入力装置は、ＩＤとなる音声を入力するものであって、マイクロホン１７からピックアップされた音声を所定の周波数ｆｏでサンプリングしてＡ／Ｄ変換し、デジタル値のビットデータを生成してその内部メモリ１６ａに記憶する。メモリ１５には、電子取引処理プログラム１５ａ、認証サーバー１３に対する認証通信処理プログ　ラム１５ｂと暗号化処理プログラム１５ｃ、そして、認証データ生成プログラム１５ｄ等が設けられている。なお、商店の端末装置１１は、いわゆる商品取扱者が操作するコンピュータであって、前記のパソコン２と同様なプログラムと構成を有しているが、ここでは、その内部は省略してある。認証サーバー１３は、送信されたデータをあらかじめ取決めてある個人ごとの暗号キーで元のデータに復元する解読回路１３ａと、送信された音声ＩＤのデータから特徴抽出処理をする特徴抽出処理回路１３ｂと、ＭＰＵ１３ｃ、そしてメモリ１３ｅとを有していて、メモリ１３ｅには、伝送された音声ＩＤの抽出された特徴パターンを記憶する音声ＩＤパターン記憶部１３１、そして、標準ＩＤパターンテーブル１３２、ＤＰマッチング処理プログラム１３３、データ送信プログラム１３４等を有している。なお、標準ＩＤパターンテーブル１３２は、多数の検索コードに対応してそれぞれの音声ＩＤの標準パターンを記憶するものであって、送信された暗号キーに対応する標準音声ＩＤパターンを検索するテーブルである。このテーブルは、ＤＰマッチング処理プログラム１３３により検索され、検索されて得られた標準パターンの１つと音声ＩＤパターン記憶部１３１のパターンデータとがＤＰ法によってマッチング処理されて、これらの一致，不一致が判定される。

【００１０】ＭＰＵ１４は、所定の条件が成立したときに電子取引処理プログラム１５ａを実行する。電子取引処理プログラム１５ａは、これが実行されると、前記の各プログラムを順次コールしてＭＰＵ１４に実行させていく。図２に従って、その処理を説明すると、電子取引処理プログラム１５ａは、個人がパソコン１２を介してインターネットの接続状態に入り、商店の端末装置１１のホームページに接続して、これから商品選択項目が選択されて図３の（ａ）に示すようなフォーマットで、商品購入情報７がインターネット１０を介してパソコン１２の画面上に得られたとする。この場合に、暗号キー入力欄６０にカーソルが位置付けられ、あるいはマウスにより指定が行われたときに割り込みスタートをする。なお、図３の（ａ）において、５０は販売元アドレス欄、５１はプロバイダ等の伝送情報欄、５２は商品番号欄、５３は数量／単価欄、５４は購入金額欄、５５は商品画像表示欄、５６は発送先住所欄／発送先コード欄、５７は氏名、電話番号等の連絡先欄、５８は届日時希望欄、５９はその他情報欄、６０は暗号キー入力欄、そして６１は音声ＩＤ入力欄である。

【００１１】ＭＰＵ１４は、まず、商品購入情報７のうち欄５９までの入力が済んだ時点で、カーソルあるいはマウスにより暗号キー入力欄６０が指定されると、電子取引処理プログラム１５ａをコールして実行する。電子取引処理プログラム１５ａの実行によりＭＰＵ１４は、まず、販売元アドレス欄５０の情報に加えて、入力された商品番号、数量、発送先住所等の欄５９までの購入情報を含めた商品購入情報７を抽出し、メモリ１５の所定の領域あるいはハードディスクの所定の領域に退避させて記憶する（ステップ１０１）。その後、認証データ生成プログラム１５ｄをコールする。ＭＰＵ１４は、認証データ生成プログラム１５ｄを実行して、まず、暗唱コード入力メッセージ等を表示してコード自体を欄６０には表示しないように処理して暗唱コードの入力を操作者にさせ（ステップ１０２）、これの入力後に続いて欄６１にカーソルをシフトさせて同様に内容表示をせずに音声ＩＤ入力をさせる（ステップ１０３）。これにより操作者が音声ＩＤとして、例えば、マイクロホン１７から「山川鳥花」という音声の入力が終了すると、キーボードのリターンキーが待ちループに入り（ステップ１０４）、キーボードからリターンキーが入力されると、ＭＰＵ１４は、音声入力装置１６のメモリ１６ａからデジタル値に変換された音声ＩＤデータを取込み（ステップ１０５）、前記の暗号キーとともにメモリ１３の所定の領域に記憶する（ステップ１０６）。

【００１２】認証データ生成プログラム１５ｄの処理が終了すると、電子取引処理プログラム１５ａは、暗号化処理プログラム１５ｃをコールして前記の音声ＩＤの「山川鳥花」を暗唱コードで暗号化したデータを生成

し、メモリ１３に記憶し（ステップ１０７）、さらに前記の商品購入情報７を暗号キーで暗号化したデータを生成し、メモリ１３あるいはハードディスクに記憶する（ステップ１０８）。なお、このとき、暗号化した各データを圧縮処理をしてもよい。次に、暗号化処理プログラム１５ｃの処理が終了すると、電子取引処理プログラム１５ａは、認証通信処理プログラム１５ｂをコールする。ＭＰＵ１４は、認証通信処理プログラム１５ｂを実行することで、送信先に認証サーバー１３を指定して図３の（ｂ）のフォーマット１８の電文を作成して（ステップ１０９）、認証サーバー１３に対するメールとしてインターネット１０に送出する（ステップ１１０）。なお、（ｂ）においては、まず、送信相手先アドレス１８ａとして認証サーバー１３のアドレスを挿入し、その後に販売元アドレス１８ｂ、販売元認証フラグ１８ｃ、発信元アドレス１８ｄ、暗唱コード１８ｅ、音声ＩＤデータ１８ｆ、ＤＬＥ（データリンクエスケープコード）１８ｇ、ＳＹＮ（同期コード）１８ｈ、そして、先にハードディスクに退避してある商品購入情報１８ｉが送出される。なお、暗唱コード１８ｄは、このとき所定の関数でスクランブル処理されたものであってもよい。

【００１３】一方、認証サーバー１３は、図４に示すように、受信割り込みスタートで処理を開始し、ＭＰＵ１３ｃの受信処理により、図３の（ｂ）のフォーマット１８の電文を受信すると（ステップ２０１）、この受信データからまず、暗号キー１８ａを抽出（スクランブル処理されているときにはスクランブルを解除）する（ステップ２０２）。なお、データ圧縮されているときには圧縮解凍をする。そして、暗唱コード１８ａをキーとして解読回路１３ａに受信データを転送して、これにより送信された受信データを復元する（ステップ２０３）。ＭＰＵ１３ｃは、次に復元データから音声ＩＤデータ１８ｃの部分を抽出して特徴抽出処理回路１３ｂに転送する（ステップ２０４）。そして、特徴抽出処理回路１３ｂにおいて転送された音声ＩＤの特徴パターンが抽出され、この特徴パターンを特徴抽出処理回路１３ｂから取込み（ステップ２０５）、それを受けてＭＰＵ１３ｃは、音声ＩＤパターン記憶部１３１に記憶する（ステップ２０６）。次に、ＭＰＵ１３ｃは、ＤＰマッチング処理プログラム１３３を実行して、音声認証処理として、暗唱コードにより標準ＩＤパターンテーブル１３２を検索して暗号キーに対応する標準パターンを読出して（ステップ２０７）、そして、これと音声ＩＤパターン記憶部１３１のデータとをＤＰ法により音声マッチング判定をする（ステップ２０８）。

【００１４】このマッチング判定で音声ＩＤが一致すると判定されたときには、ＭＰＵ１３ｃは、受信データの販売元認証フラグ１８ｃを参照してここにフラグが立てられいるか否かを判定し（通常はフラグを立てるものとする）、これにより商店の端末装置１１について認証するか否かの判定をする（ステップ２０９）。最初は、ここでＹＥＳとなり、前記の認証フラグをリセットして（ステップ２１０）、受信データの販売元アドレス１８ｂを抽出して（ステップ２１１）、商店の端末装置１１に対して注文ありの電文とともに所定のフォーマットに従って音声ＩＤと暗唱コードの入力をして送信することを促すメッセージの電文を伝送を送出する（ステップ２１２）。そして、受信待ちにループに入る（ステップ２１２）。これにより商品取扱者の音声ＩＤによる認証処理を行う。なお、受信データの販売元認証フラグ１８ｃがリセットされた状態で受信したときには、前記のステップ２０９の判定でＮＯとなるので、後述するステップ２１４において認証サーバー１３が商店の端末装置１１に商品購入情報７を送出することになる。購入者はこの販売元認証フラグをリセットする選択ができるものとする。さて、商店の端末装置１１から音声ＩＤと暗唱コードを受けると、この音声ＩＤと暗唱コードについて認証をするために前記のステップ２０１へと戻り、ステップ２０１からステップ２０７を経て、ステップ２０８の判定で音声ＩＤが一致しているとされたときには、今度は、ステップ２０９の認証フラグ判定でＮＯとなる。そこで、入力された商品番号、数量、送り先アドレス等の購入情報を含めた商品購入情報７が発信元を認証サーバー１３としてインターネット１０を介して商店の端末装置１１に送出する（ステップ２１４）。なお、音声マッチング判定で不一致のときには、発信元アドレス１８ｄに従ってアクセス拒否，再送要求応答が発信元に送出される（ステップ２１５）。

【００１５】このようにすることで、商店の端末装置１１は、発信元が認証サーバー１３であるときには、個人認証が完了しているものとして、商品を安心して発送できる。また、認証サーバー１３は、このとき、商店の端末装置１１と購入者との間に第三者として介在し、かつ、音声ＩＤという個人特有の特徴により認証を行うので、安全性の高い照合ができる。その結果、電子商品取引システムの信頼性を向上させることができ、さらに、認証サーバー１３から音声ＩＤ認証を行った個人のデータと送信されたデータから金額等を抽出して暗唱コードとともにクレジット会社に送信して金額引き落としの決済の送信をして即座にオンライン決済することができる。

【００１６】ところで、この実施例のように専用の認証サーバーを設けることで、認証情報のデータ量は、ＩＣカードよりも多くの容量を割り当てることができる。これにより、秘密性を向上させ、データの信頼性を高めることができる。そこで、各商店の端末装置１１やパソコン１２に備える認証のための入力装置としては、操作者の身体的特徴として、音声ＩＤばかりではなく、例えば，声紋入力手段により声紋を入力し、認証サーバー１３により声紋を比較判定するようにしてもよい。すなわ

ち、入力された声紋は、暗号化手段によって暗号化された後に、一般のネットワーク経由で認証サーバー１３に転送される。認証サーバー１３は、受信した暗号化声紋を復号化手段で復号化して入力声紋情報を得る。そして、同時に受信した操作者の暗号コード（操作者のＩＤ）に基づいて照合手段を用いて登録済みの声紋ファイルから当該操作者の声紋を抽出して入力声紋と比較照合し、合致したら本人と見なす処理をする。なお、一般のネットワークを利用してデータを送信する関係での暗号化としては、前記の暗号コードによるもののほかに、操作者ごとに予め設定した、例えば、秘密キー、可変キーなども加えて暗号処理をして、これらのキーとともに伝送情報を認証サーバー１３に送信するようにしてもよい。

【００１７】この場合には、認証サーバー１３は、送信された秘密キー、可変キーなどを解読キーとして利用する。例えば、声紋等の復号化にあたっては秘密キーに対応した公開キーを公開キーファイルから暗号コードに基づいて抽出して用いることができる。可変キーとしては、例えば、日時など、暗号結果を毎回異ならせて、送信中に仮に盗まれても、毎回結果が異なるようにして、単純に複製しても不正利用できないようにすることができる。

【００１８】以上説明してきたが、実施例では、購入者のパソコンと商品取扱者（販売者）の端末装置とは直接データの授受を行う接続がなされることはなく、データが相互伝送されることはない。商品の購入のときには、認証サーバーが介在して購入情報のデータが商品取扱者に伝送される。また、商品購入の際にも購入者のパソコンは、認証が正しいときには、単に認証サーバーにデータを伝送するだけになる。また、ネットワークに接続される装置は、パソコンのみならず電話機や携帯電話機やＰＨＳやＰＤＡやインターネットＴＶなどであってもよい。また、電子化された身体的特徴は、声紋のみならず角膜紋、指紋、指の骨形状、顔面パターンなど、個人の特徴を識別できるものであればよい。さらに、ネットワークは、有線，無線を問わずまた電話網、通信回線、ＣＡＴＶ、衛星通信などでもよい。暗号化手段や復号化手段は公開鍵方式、秘密鍵方式のいずれでもよい。

【００１９】

【発明の効果】この発明にあっては、暗唱コードなどのパスワードを用いずに身体的特徴を用いることで、認証のためのデータ量が多くなる。それだけ認証データの解読がし難くなり、また、身体的特徴である関係からその人特有の情報になる。さらに、認証サーバー等の第３の情報処理装置に第三者機関として配置し、身体的特徴の情報を認証情報として商品購入情報と合わせて伝送するようにしているので、商品取引と本人確認とが第三者機関を介在して行われることになるので信頼性が増加する。特に、身体的特徴の情報と検索コードの伝送情報は、第２の情報処理装置（商品購入者）から第３の情報処理装置（認証サーバー）と一方的に流れる伝送になっていて、さらに、購入情報も認証サーバーから第１の情報処理装置（商品取扱者）と一方的に流れる伝送であるので、商品購入者と認証サーバーとの間だけで特殊な暗号化によりデータ送信ができる。また、商品の販売者（商品取扱者）と認証サーバーとの間でも必要な場合には別な暗号化も可能であり、ここでは購入者の身体的特徴の情報や検索コードの情報伝送は不要になる。また、ＩＣカードのように、第１の情報処理装置と第２の情報処理装置あるいは第３の情報処理装置と第２の情報処理装置との間で個人確認されたことについてのデータの授受をしなくても済むので、信頼性が向上する。その結果、従来のＩＣカード等を利用したパスワード方式に比べ大幅な機密の向上を図ることができる。さらに、身体的特徴の照合を操作手段側にて行わないずに、第三者の認証サーバー等の第３の情報処理装置で行うことにより、インターネットなどのような利用相手を限定できないオープンな公衆ネットワークにおいて信頼性の高い電子商品取引を行うことができる。

【図面の簡単な説明】

【図１】図１は、この発明の電子商品取引システムのインターネットを利用した一実施例のブロック図である。

【図２】図２は、電子商品取引処理の購入者側装置の処理のフローチャートである。

【図３】図３は、電子取引における商品購入フォーマットの一例の説明図であって、（ａ）は、その表示画面における入力フォーマットの説明図、（ｂ）は、そのデータ伝送フォーマットの説明図である。

【図４】図４は、電子商品取引処理における認証サーバーの処理のフローチャートである。

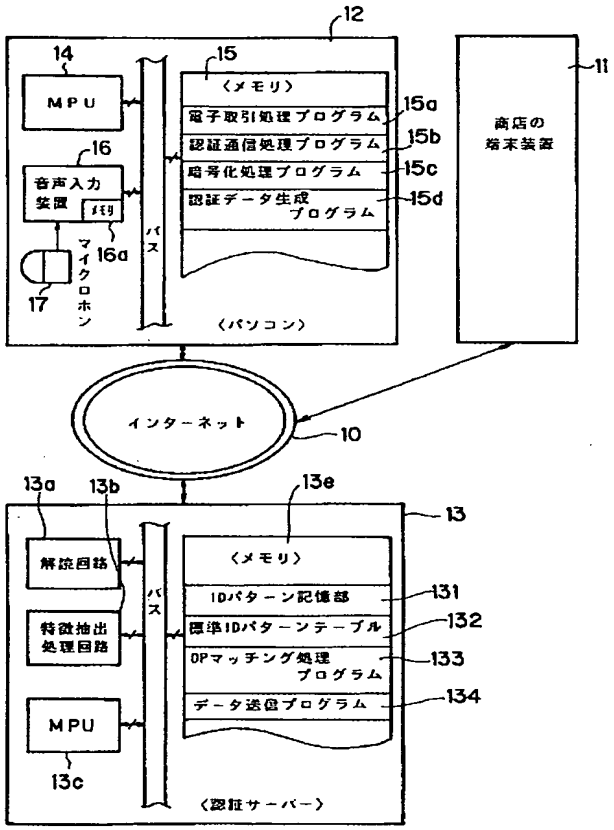
【図５】図５は、インターネットを利用した電子商品取引システムの全体的な構成図である。

【図６】図６は、インターネットを利用した従来の電子商品取引システムの説明図である。

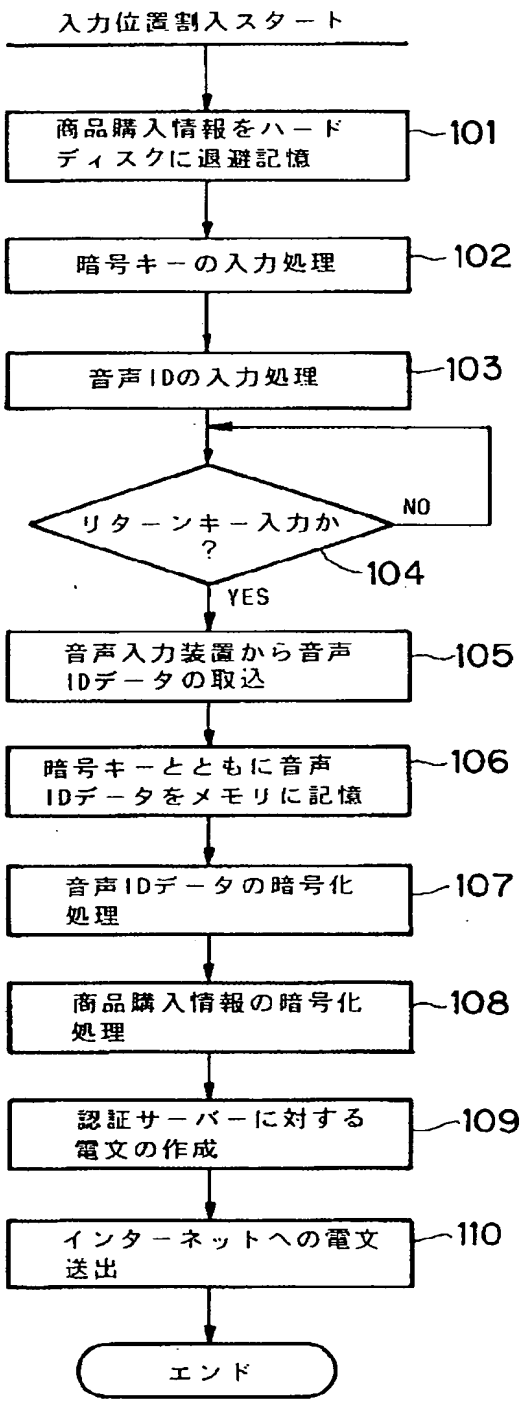
【符号の説明】

１…予約販売会社のサーバー、３…ＩＣカード、１０…インターネット、１１…商店の端末装置、２，１２…パーソナルコンピュータ（パソコン）、４，１３…認証サーバー、１３ａ…解読回路、１３ｂ…特徴抽出処理回路、１３ｅ，１５…メモリ、１３１…音声ＩＤパターン記憶部、１３２…標準ＩＤパターンテーブル、１３３…ＤＰマッチング処理プログラム、１３４…データ送信プログラム、１３ｃ，１４…ＭＰＵ、１６…音声入力装置、１７…マイクロホン、１５ａ…電子取引処理プログラム、１５ｂ…認証通信処理プログラム、１５ｃ…暗号化処理プログラム、１５ｄ…認証データ生成プログラム。

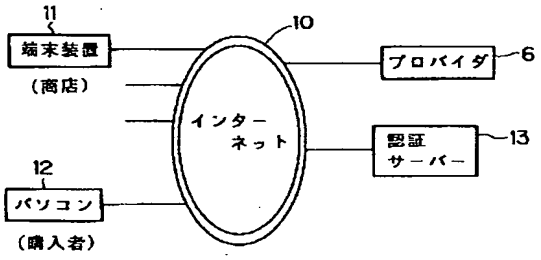
【図１】


12
14
15
MPU
〈メモリ〉
15a
電子取引処理プログラム
15b
認証通信処理プログラム
15c
暗号化処理プログラム
15d
認証データ生成プログラム
16
音声入力装置
16a
マイクロホン
17
バス
〈パソコン〉
11
商店の端末装置
インターネット
10
13a
13b
13e
13
解読回路
特徴抽出処理回路
MPU
13c
〈メモリ〉
IDパターン記憶部
131
標準IDパターンテーブル
132
DPマッチング処理プログラム
133
データ送信プログラム
134
〈認証サーバー〉

【図２】

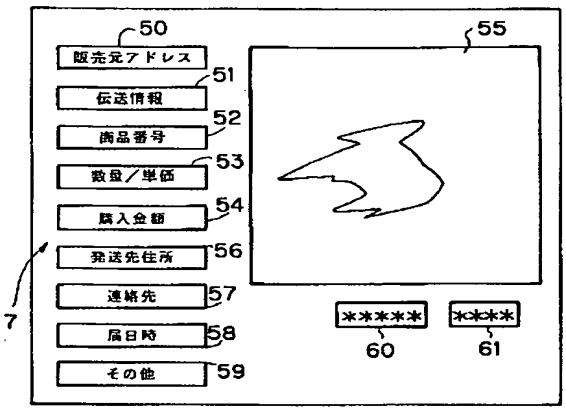

入力位置割入スタート
商品購入情報をハードディスクに退避記憶
101
暗号キーの入力処理
102
音声IDの入力処理
103
リターンキー入力か？
NO
104
YES
音声入力装置から音声IDデータの取込
105
暗号キーとともに音声IDデータをメモリに記憶
106
音声IDデータの暗号化処理
107
商品購入情報の暗号化処理
108
認証サーバーに対する電文の作成
109
インターネットへの電文送出
110
エンド

【図５】

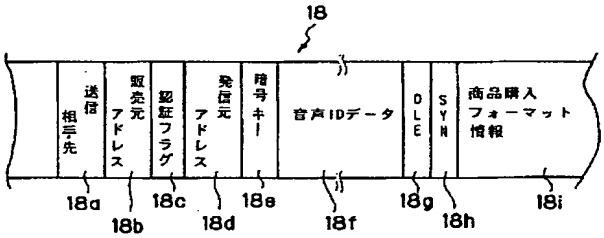

11
端末装置
（商店）
12
パソコン
（購入者）
10
インターネット
プロバイダ
6
認証サーバー
13

【図３】

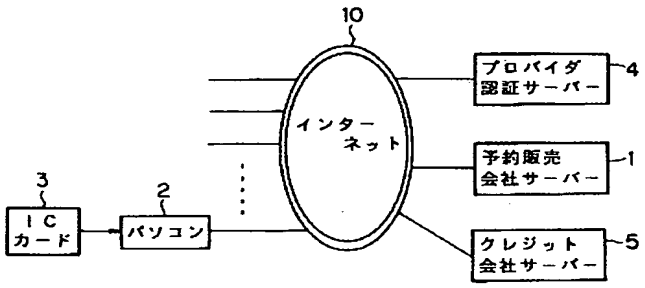
(a)


販売元アドレス
伝送情報
商品番号
数量／単価
購入金額
発送先住所
連絡先
届日時
その他
50
51
52
53
54
55
56
57
58
59
7
*****
****
60
61

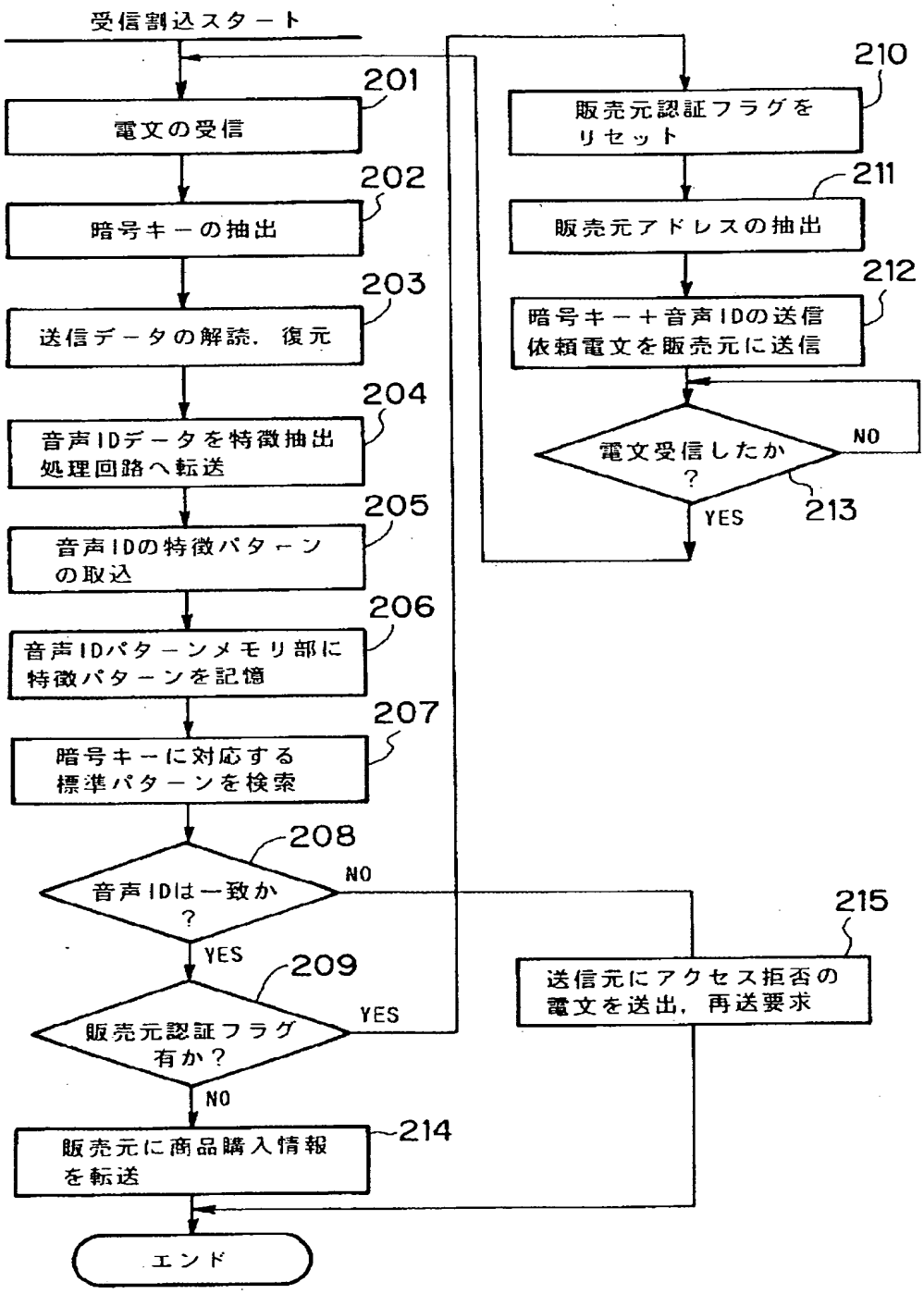
(b)


18
送信相手先
販売元アドレス
認証フラグ
発信元アドレス
暗号キー
音声IDデータ
DLE
SYN
商品購入フォーマット情報
18a
18b
18c
18d
18e
18f
18g
18h
18i

【図６】


10
インターネット
プロバイダ認証サーバー
予約販売会社サーバー
クレジット会社サーバー
4
1
5
3
ICカード
2
パソコン

【図４】


受信割込スタート
201
電文の受信
202
暗号キーの抽出
203
送信データの解読，復元
204
音声IDデータを特徴抽出処理回路へ転送
205
音声IDの特徴パターンの取込
206
音声IDパターンメモリ部に特徴パターンを記憶
207
暗号キーに対応する標準パターンを検索
208
音声IDは一致か？
NO
YES
209
販売元認証フラグ有か？
YES
NO
214
販売元に商品購入情報を転送
エンド
210
販売元認証フラグをリセット
211
販売元アドレスの抽出
212
暗号キー＋音声IDの送信依頼電文を販売元に送信
電文受信したか？
NO
YES
213
215
送信元にアクセス拒否の電文を送出，再送要求